IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Application of Melissa W. Dunn Art Unit 2154
Serial No. 10/084,859
Filed February 27, 2002
Confirmation No. 8746
For SYSTEM AND METHOD FOR USER-CENTRIC AUTHORIZATION TO ACCESS USER-SPECIFIC INFORMATION
Examiner Joshua Joo

December 18, 2007

RESPONSE TO NOTIFICATION OF NON-COMPLIANT APPEAL BRIEF

SUBMITTING SUMMARY OF CLAIMED SUBJECT MATTER

TO THE COMMISSIONER FOR PATENTS,

SIR:

In response to the Notification of Non-Compliant Appeal Brief, dated November 25, 2007, please replace the Summary of Claimed Subject Matter, which begins at page 2 of the Appeal Brief, with the following **Amended Summary of Claimed Subject Matter**, which begins on page 2 of this paper.

V. AMENDED SUMMARY OF CLAIMED SUBJECT MATTER

The following summary correlates claim elements to embodiments described in the application specification, but does not in any manner limit claim interpretation. Rather, the following summary is provided only to facilitate the Board's understanding of the subject matter of this appeal.

According to aspects of the present invention, web-services users 202 control access to their user-specific information stored with a web-services service by access control settings. (Application, page 11, lines 1-15). The web-services client determines dynamically whether to grant or deny an access request that does not comply with default access control settings. Advantageously, the present invention rests the burden of managing intentions with each web-services client. Stated differently, the present invention places no additional burdens on the authorization and authentication mechanisms used by the web-services provider. *See* Application, pages 16-22, 41 (lines 8-20) and FIG. 2.

In this regard, claim 29 is directed to a system for controlling access to user-specific information in a network computing environment. As described in the application and illustrated in FIG. 2, aspects of the invention include a web-services service provider 204, a user 202 of a service (#1 to #n) of the web-services provider 204, a client 220 of the web-services provider 204, an access control engine 232 and a consent engine 236. (Application, FIG. 2). The web-services provider 204 maintains a data store of user-specific information associated with the user 202. (Application, page 17, lines 7-9). The user-specific information is accessible by the user 202. Accessed by the client 220 is controlled by the user 202. (Application, page 19, lines 25-30). A set of default access preferences 234 define a list of default access permissions 210, 216 that are allowed by the user 202. (Application, page 21, lines 1-8).

The client 220 generates a request to access to certain of the user-specific information associated with the user 202. (Application, page 22, lines 2-5). The request identifies an intended use by the client 220 of the certain user-specific information in the data store. (Application, page 22, lines 5-6).

The access control engine 232 receives the client request to access the certain user-specific information and dynamically creates an access control rule by comparing the set of default access preferences with the intended use by the client. (Application, page 22, lines 6-9). The access control rule grants the requested access by the client to the certain user-specific

information if the intended use of the client of the certain user-specific information is within the list of default access permissions defined by the set of default access preferences defined by the user 202. (Application, page 22, lines 9-11).

The consent engine 236 generates an option list in response to the client's request for user-specific information when the intended use is outside the list of default access preferences defined by the user 202. (Application, page 30, lines 11-16; page 30, line 30 - page 31, line 2). The option list contains at least one entry based on the intended use by the client of the user-specific information in the data store. (Application, FIG. 3). The consent engine 236 displays on the display interface of the network communication device an option menu reflecting the generated option list. (Application, page 30, line 30 - page 31, line 2). The option menu prompts the user to accept or reject at least one option displayed on the option menu using the selection interface of the network communication device. (Application, page 35, lines 11-13; ~~See Application, pages 34, 35 and~~ FIGS. 5A, 5B).

Claim 15 is directed to a method of controlling access to user specific information for use in a network computer system including a web-services provider, a user of a service provided by the web-services provider, and a client of the web-services provider. (Application, FIG. 2). The web-services provider receives a request from the client to access the certain user-specific information in the data store of user-specific information associated with the user. (Application, page 22, lines 2-5; FIG. 6, reference character 648). The user-specific information is accessible by the client controlled by the user. (Application, page 19, lines 25-30). The client generates an intended use request to certain user-specific information in the data store. (Application, page 24, lines 22-26). The web-services provider determines an allowed level of access permitted by the user and compares the generated intended use request with the determined allowed level of access. (Application, page 25, lines 1-4; FIG. 6, reference character 652). If the generated intended use request is outside the allowed level of access, a consent engine is invoked. (Application, page 25, lines 22-26; FIG. 6, reference character 614). The consent engine informs the user of the client's request to access the certain user-specific information in the data store and invites the user to permit or to deny the client's request to access the certain user-specific information. (Application, page 22, lines 24-30, FIG. 6, reference characters 672, 674; FIG. 3). When the generated intended use request by said client of the certain user-specific information is within the determined allowed level of access permitted by the user, the web-services provider

completes the request from the client to access the certain user-specific information in the data store. (Application, page 21, lines 16-19; FIG. 6, reference characters 654, 658, 660, 636, 646, 662, 664, 626).

As further illustrated in FIG. 7 and the corresponding descriptions in specification, such as page 41, embodiments of the invention places the burden of managing intentions on each web-services client. (Application, page 41; FIG. 7). This advantage places no additional burdens on the authorization and authentication mechanisms used by the web-services provider and a separate service-side fabric is not required.

REMARKS

Applicants submit that the Appeal Brief, as corrected by the Amended Summary of Claimed Subject Matter submitted herewith, is now in compliance with 37 CFR 41.37(c)(1)(v) and respectfully request a substantive evaluation of the issues presented.

Respectfully submitted,

/Frank R. Agovino/

Frank Agovino, Reg. No. 27,416
SENNIGER POWERS
One Metropolitan Square, 16th Floor
St. Louis, Missouri 63102
(314) 231-5400